http://Lafox.Net

Alice Lafox

alice@lafox.net

Oleg Tsymaenko

tsyma@lafox.net

Yury Timoshevsky

nexus@lafox.net

http://Lafox.Net
Alice Lafox, Oleg Tsymaenko, Yury Timoshevsky

Опубликовано 2003-09-10

История переиздания

Издание 0.1 16-08-2003 Revised by: al
Starting manual

Содержание

Предисловие

1. Юридическое замечание

2. О нас

Lafox.Net[2] распространяет свободное программное обеспечение. Lafox.Net[3] таким образом вносит свой вклад в популяризацию и распространение операционной системы `GNU/Linux`.

Кроме распространения свободного программного обеспечения на CD-дисках, команда Lafox.Net[4] активно занимается развитием *Mandrake Linux*. В частности, мы поддерживаем русскую версию сайта *Mandrake Linux* http://www.mandrakelinux.com/ru/, делаем переводы на русский документации http://www.mandrakelinux.com/ru/fdoc.php3[6], принимаем участие в написании англоязычной документации по *Mandrake Linux*, а также в локализации *Mandrake Linux*.

3. Зачем нужно это руководство

Lafox.Net[7] занимается распространением свободного программного обеспечения, а также некоторой поддержкой пользователей Linux. Нам часто приходится отвечать на однотипные вопросы. Данный процесс привел нас к мысли создать данную книгу.

Эта книга является сборником типовых решений для наиболее часто встречающихся задач под *Mandrake Linux*. Таким образом, эту книгу можно рассматривать как несколько расширенные FAQ по *Mandrake Linux*. Книга содержит прямые указания по настройке и использованию *Mandrake Linux* в качестве рабочей станции и сервера. Мы постарались удержаться от приведения теории и описания редко используемых функций и приводить только описание действий для быстрой типовой настойки. Эта книга скорее являет собой набор пошаговых инструкций.

Мы постарались воздержаться также от описания инструментальных средств настройки, отдав предпочтение описанию всех действий через утилиты командной строки и прямое редактирование конфигурационных файлов. Мы считаем, что такой подход лучше, так как он: во-первых, короче в изложении, а во-вторых, меньше привязан к операционной системе. Исходя из этого, практически все, описанное в этой книге (кроме процесса инсталляции и способов установки пакетов, а также, в некоторых случаях, путей к файлам и каталогам), вполне справедливо и для систем, отличных от *Mandrake Linux*. Все, что касается настройки сервисов (демонов), можно смело применять для других дистрибутивов `GNU/Linux`, а также для других `UNIX` систем, таких как FreeBSD.

Целью руководства является не обучение работе с `GNU/Linux`, а быстрая, в течении 1-2 часов, настройка системы и основных сервисов. Мы планируем постоянно расширять и дополнять это руководство. Свежую версию всегда можно получить на http://lafox.net/docs/. Мы также создали на нашем форуме поддержки специальный раздел для обсуждения этой книги (http://lafox.net/support/). В этом форуме можно (и нужно) оставлять заявки на новые разделы книги, а также указывать на все неточности, которые вам "посчастливилось" обнаружить. Мы будем благодарны за отзывы и предложения.

Итак, задача состоит в следующем:

1. http://www.gnu.org/licenses/fdl.html
2. http://Lafox.net/
3. http://Lafox.net/
4. http://Lafox.net/
6. http://www.mandrakelinux.com/ru/fdoc.php3
7. http://Lafox.net/

- Есть: инсталляционные диски Linux Mandrake 9.1-9.2
- Нужно: установить полноценную рабочую станцию с хорошей русификацией, а также сетевой сервер, который будет заниматься такими вещами, как:
  - выполнять функции DNS сервера (named);
  - выполнять функции маршрутизатора и заниматься "раздачей" internet трафика во внутреннюю сеть (IPMASQUARADE);
  - выполнять функции кэширующего прокси сервера для HTTP трафика (`Squid`);
  - выполнять функции корпоративного FTP сервера (ProFTPD);
  - выполнять функции корпоративного файлового сервера (`Samba`);
  - выполнять функции корпоративного почтового SMTP сервера (`Postfix`);
  - выполнять функции корпоративного почтового pop3/pop3s/imap/imaps сервера (IMAP);
  - выполнять функции корпоративного Web сервера (`Apache`).

Начнем пожалуй, с установки системы:

Глава 1. Пошаговые инструкции

У вас должно быть 3 инсталляционных диска с *Mandrake Linux* 9.1-9.2 и приблизительно 3GB свободного места на жестком диске (это может быть полностью неиспользованный раздел или место, вообще не занятое разделами). В BIOS вашего компьютера рекомендуется проставить PNP OS Installed = NO или OFF. Добиваемся того, чтобы компьютер мог загружаться с CD-ROM. Включаем все периферийное оборудование (принтеры, сканеры, модемы и тд): это необходимо для того, чтобы программа установки нашла их в процессе инсталляции.

Вставляем первый диск (Installation CD1) и грузимся с него.

При загрузке сразу появится графическая заставка с вопросом: F1-для дополнительных опций или ENTER для инсталляции или обновления. Нажимаем ENTER и дожидаемся загрузки графического интерфейса инсталлятора. Далее следуют пошаговые инструкции:

1. Language: выбор языка. Выбираем: *Europe -> Русский*. и жмем **Далее ->**. Если нужна поддержка украинского, все равно выбираем русский (о том, как сделать поддержку украинского вы узнаете в главе Гл. 2).
2. Лицензия: выбираем **Принять** и жмем кнопочку **Далее ->**. Разумеется, что если вы первый раз устанавливаете *Mandrake Linux*, или вам просто интересно, тогда можете ее и почитать **:-)**.
3. Тип Мыши:- выберите свой. Чаще всего это PS/2 -> стандартный или PS/2 -> стандартная мышь с колесиком. В большинстве случаев здесь вообще ничего менять не надо. Жмем **Далее ->**.
4. Раскладка клавиатуры: оставляем Русская. Жмем **Далее ->**.
5. Горячие клавиши переключения раскладки клавиатуры: выбираем то, к чему привыкли, например, Ctrl+Shift. Жмем **Далее ->**.
6. Уровень безопасности и email куда будут посылаться отчеты по безопасности: пока оставим стандартный и введем email admin. Жмем **Далее ->**.
7. Выбор типа разметки диска: выберем ручная. Далее выбираем свободное место (белого цвета) и создаем нужные разделы. В простейшем случае требуются только "/" и "swap". Размер "swap" рекомендуется выбирать примерно 2*RAM, то есть если у вас 128MB памяти, то swap возьмите ~250-300MB. В случае использования Linux как сервера, рекомендуется создать также разделы /var и /home, а также сделать отдельными разделами те места, которые могут быть переполнены пользователями, работающими сервисами или лог файлами. Например:
   - /var/log: сюда пишутся системные логи и логи большинства сервисов;
   - /var/ftp: здесь размещаются файлы, распространяемые по FTP;
   - /var/www: здесь размещаются ваши web- сайты;
   - /var/spool/mail: здесь размещаются почтовые ящики ваших пользователей;
   - /usr/local: этот раздел можно создать отдельным, если вы намереваетесь устанавливать с помощью компиляции дополнительный софт и хотите чтобы он был доступен после переустановки системы;
   - /var/spool/squid/: здесь лежит кэш прокси- сервера Squid;
   - /var/lib: здесь многие сервисы, например, сервера баз данных MySQL и Postgres, хранят файлы баз данных.

   Напоминаем, что эти разделы делать необязательно, особенно для рабочей станции. Размеры этих разделов выбирайте самостоятельно, исходя из задач настраиваемого сервера и размера вашего диска.
8. Выбор групп пакетов: ставим все галочки, кроме другие графические рабочие столы и Выбор отдельных пакетов.

Замечание: Важно включить *ВСЕ*, что касается серверов и сетевых рабочих станций, а также LSB и разработки. Еще лучше отметить все разделы, не выбирая опции выбор отдельных пакетов. Полная инсталляция в этом случае будет занимать примерно 2GB. В случае, если вы устанавливаете сервер, вы можете отключить все что касается игр, офисных приложений, а также GNOME и KDE. Хотя установка, например KDE, работе сервера не помешает **:-)**.

Жмем **Далее ->**.

9. Инсталлятор задает вопрос о необходимости установки некоторых серверных программ, таких как ProFTPD, Postfix, bind и т.д.. Отвечаем `Да` и жмем кнопочку **Далее ->**.
10. Наслаждаемся процессом установки (~10-60 мин в зависимости от производительности компьютера). В ходе установки, по требованию инсталлятора, вставляем 2-ой диск (`Installation CD2`) и 3-й диск (`International CD`).
11. `Пароль root`: введите дважды пароль суперпользователя системы. `root` - это суперпользователь в системах UNIX, чем-то напоминает "Администратор" в M$ Window$ NT/2000/XP. При выборе пароля рекомендуется следовать следующим правилам: пароль не должен быть словом из словаря или какими-то личными данными владельца (не марка автомобиля и не дата рождения а таже не word). Пароль должен содержать большие и маленькие буквы и, желательно, также цифры. При этом пароль должен быть легко запоминаемым, для того чтобы вам не требовалось его записывать. [1]

    Как пример генератора хороших паролей можем привести http://lafox.net/utils/pwgen/[2].

    Жмем **Далее ->**.

12. Добавляем обычного пользователя. Пусть это будет `admin`. Желательно, чтобы пароль не совпадал с паролем суперпользователя `root` и выбирался по таким же правилам, как и для `root`. Обратите внимание, что в UNIX-системах (и в Linux) имена пользователей и их пароли регистрозависимые. То есть пользователь с логином `admin` и пользователь с логином `Admin` - это два совсем разных пользователя.
13. `Автоматический вход в систему`: рекомендуем отключить эту возможность, особенно если настраиваемый вами компьютер будет выполнять функции сервера, или если вы собрались хранить на нем что либо важное. При таком режиме любой человек, включивший в вашем отсутствии компьютер, сразу без ввода пароля получит доступ ко всем вашим программам и данным. На сервере это вообще недопустимо.
14. `Установка начального загрузчика`: выберите `Первый сектор диска (MBR)`. Это не лучший вариант, но при отсутствии опыта - самый простой и надежный. [3]
15. `Сводка`: здесь нужно остановится более детально.
    - `Система -> Часовой пояс`: вместо `Europe/Moscow` выбираем `Europe/Kiev`, если вы живете на Украине. Потом снимаем галочку `аппаратные часы выставлены по GMT`.
    - `Оборудование -> Графический интерфейс`: выберите здесь свою видеокарту. Обычно инсталлятор сам определяет тип видеокарты и монитор (в большинстве случаев plug'n'play), поэтому скорее всего ничего менять здесь не прийдется.
    - `Boot -> сервисы`: нажимаем левую нижнюю кнопочку **Развернуть дерево** и убираем все лишнее. Ниже помечены звездочкой * сервисы, которые используются только на сервере. В случае настройки рабочей станции их тоже можно отключать. Итак, оставляем выбранными следующие сервисы:
        - `alsa` - расширенная звуковая архитектура в Linux (конечно, если у вас есть SoundCard);
        - `atd` - позволяет запускать задания в определенное время;
        - `cron` - планировщик заданий (аналог шедуллера в M$ Window$);
        - `harddrake` - отслеживает изменения в конфигурации компьютера;
        - `keytable` - загружает русскую раскладку клавиатуры;
        - `kheader` - можно оставить, особенно если вы будете часто использовать заголовочные файлы ядра;
        - `network` - запускает сетевые интерфейсы;

---

1. Программы по взлому паролей сначала перебирают варианты из словарей. Человек, подбирающий пароли, в первую очередь пытается попробовать слова, как-то связанные лично с вами, например, имя вашей собаки или название вашей улицы. Человек, старающийся похитить ваш пароль, в первую очередь осмотрит ваше рабочее место на предмет записанных паролей. Огромное число взломов произошло из-за того, что пользователи записывали свой пароль на коврике для мыши или мониторе.
2. http://lafox.net/utils/pwgen/
3. В идеале загрузчик нужно ставить в "Первый сектор корневого раздела". Но в этом случае существует большая вероятность того, что Linux по окончанию установки не загрузится. Для поправления этого нужно загрузится с первого CD-диска инсталляции в rescue mode, а потом программой fdisk проставить корневому разделу флажок "A". Кроме того, в таком варианте корневой раздел должен быть Primary.

- `random` - переинициализирует системный генератор случайных чисел;
- `rawdevices` - оставить в случае, если у вас есть DVD;
- `sound` - звук. Настраивает микшер и т.д.;
- `syslog` - служба, с помощью которой, многие приложения пишут log файлы;
- `xfs` - сервер шрифтов (нужен для `X`);
- `xinetd` - запуск некоторых сервисов, таких как POP3
- `devfsd` - поддержка сменяемых по горячему устройств (например USB цифровых камер);
- `dm` - запуск графической оболочки `X`;
- `named` * - DNS сервер;
- `postfix` * - почтовый SMTP сервер;
- `cups` - сервер печати. Нужен, если вы пользуетесь принтером (как локальным, так и сетевым);
- `httpd` * - HTTP (WWW) сервер Apache2
- `iptables` - файервол (брандмауэр). В нашем случае нужен для "раздачи" интернет;
- `proftpd` * - FTP сервер;
- `netfs` - монтирует удаленные сетевые файловые системы (полезно);
- `smb` * - файловый сервер `Samba`
- `sshd` * - защищенный удаленный доступ к командной строке вашего компьютера.

- Если вам необходимо, настройте также `оборудование -> звуковая карта` и `оборудование -> принтер`.
- `Настройка сети`:
  - Включаем `Использовать автоопределение` и `Режим Эксперта`. **Далее ->**
  - Выбираем `Соединение по локальной сети`. **Далее ->**
  - Говорим что больше нет никаких устройств (выбрать **NO**). **Далее ->**
  - Указываем здесь IP и маску подсети. **Далее ->**
  - Вводим имя хоста, DNS сервер и основной шлюз (`Default GateWay`). **Далее ->**
  - `HTTP Proxy` и `FTP Proxy` пока оставим пустыми. **Далее ->**

  На этом пока все. Более подробным настройкам сети мы посвятим отдельный раздел чуть позже.

  Возвращаемся в раздел `сводка` и нажимаем **Далее ->**..

16. `Установка обновлений`: на вопрос об установке обновлений отвечаете `НЕТ` (разумеется, если вы не желаете выкачать 200-500Mb иностранного трафика).
17. Установка закончена. Жмем **Перезагрузка** и ждем пока машина перезагрузится. Не забудьте вытащить диск из CD-ROM и восстановить в `BIOS` загрузку с жесткого диска.

Глава 2. После инсталляции: обработка напильником

2.1. Настройка MidNight Commander (mc).

В UNIX системах считается дурным тоном пользоваться подобными файловыми менеджерами. Но, при переходе от M$ Window$, многим будет приятно получить в распоряжение файловый менеджер, чем-то напоминающий far/nc/dn/vc ....

- Вызываем терминал (например, `Konsole` - в `KDE` третья слева внизу иконка)
- Получаем права пользователя root (или становимся root)

  ```
  $ su -l
  ```

- Устанавливаем MidNight Commander

  ```
  # urpmi mc
  ```

- Возвращаемся из режима root в своего пользователя

  ```
  # exit
  ```

  или просто Ctrl+D и просто запускаем mc:

  ```
  $ mc
  ```

- В нем сразу включаем: *меню -> настройки -> биты символов -> Полный 8-битный ввод*. Это необходимо для того, чтобы появилась возможность ввода русских букв. Теперь там же в настройках *меню -> настройки -> биты символов -> Кодировка ввода/вывода* выбираем `KOI8-U` [1]. Это нужно для того, чтобы в редакторе (mcedit) появилась возможность редактировать файлы в различных кодировках (таких как cp1251 или cp866). Эту возможность можно вызывать в редакторе (mcedit) комбинацией клавиш Ctrl+T.
- Все это сохраним *меню -> настройки -> сохранить настройки*.
- Пользуемся :)

2.2. Настройка переключения раскладки клавиатуры для X

В файлике `/etc/X11/XF86Config-4` секцию `InputDevice` нужно привести примерно к такому виду:

```
Section "InputDevice"
    Identifier "Keyboard1"
    Driver "Keyboard"
    Option "XkbModel" "pc105" #тут оставить свое
    Option "XkbLayout" "us,ru(winkeys),ua(winkeys)" # для 3-х языков (eng,rus,ukr)
#   Option "XkbLayout" "us,ru(winkeys)" # для 2-х языков (eng,rus)
    Option  "XkbOptions" "grp:ctrl_shift_toggle,grp_led:scroll" # индикатор ScrollLock
EndSection
```

В приведенном примере также разблокируется доступ к виртуальным текстовым консолям по CTRL+F1, CTRL+F2 ....

Если нужно только 2 языка, снимите комментарий со строки

```
#   Option "XkbLayout" "us,ru(winkeys)"
```

и закомментируйте строку

```
Option "XkbLayout" "us,ru(winkeys),ua(winkeys)"
```

Не забудьте перед внесением изменений сделать резервную копию файла `/etc/X11/XF86Config-4`. Это можно сделать следующей командой:

1. Кодировка `KOI8-U` содержит в себе все символы `KOI8-R` плюс все украинские символы. Полезно выбирать ее, если вам нужен так же и украинский язык.

```
# cp -f /etc/X11/XF86Config-4 /etc/X11/XF86Config-4.backup
```

Не забудьте после внесения изменений перезагрузить X-сервер. Для перезапуска X-server закройте все приложения и нажмите CTRL+BackSpace.

2.3. Установка шрифтов M$ Window$

- Если у вас есть раздел (fat/ntfs) с установленным M$ Window$ тогда используем команду

  `# drakfont --strong -wi`

- Если у вас нет установленного M$ Window$ или вы хотите явным образом задать каталог где лежат шрифты то используйте команду

  `# drakfont --strong --install /path/to/fonts/*.ttf`

  и также если вам нужно установить один шрифт то вместо /path/to/fonts/*.ttf пропишите полный путь к файлу шрифта.

- Также можно запустить эту утилиту для визуального управления шрифтами.

> **Замечание:** Внимание!!! Установка всех подряд шрифтов, имеющихся в M$ Window$, не всегда проходит успешно. Бывает так, что при наличии дополнительных шрифтов от третих производителей возникают проблемы с использованием этих шрифтов под Linux. Поэтому мы собрали и разместили самые необходимые и работающие шрифты здесь: http://lafox.net/files/ttf.tar.bz2. Размер приблизительно 5.2Mb.

Глава 3. Настройка DNS сервера

3.1. Кеширующий DNS сервер;

Кеширующий DNS сервер может понадобится как DNS сервер в локальной сети. При наличии кеширующего DNS на вашем сервере сети все компьютеры в сети смогут использовать ваш сервер как DNS. Кроме того это несколько ускоряет распознование доменных имен и часто используется даже при использовании Linux как рабочей станции. Приступим к настройке:

Провеяем что установлены (или устанавливаем) пакеты bind и bind-utils:

```
#urpmi bind bind-utils
```

Пусть 222.222.222.222 - это IP-адрес сервера DNS вашего провайдера.

Теперь вносим изменения в файле `/etc/named.conf` в секции "options". Нужно добавить следующие строки:

```
forwarders { 127.0.0.1; 222.222.222.222; };
forward first;
```

Далее правим файлик `/etc/resolv.conf` - в нем должны быть строки:

```
nameserver 127.0.0.1
nameserver 222.222.222.222
```

Это может понадобится для некоторых служб и программ которые не будут обращаться к вашему DNS серверу.

После этого перезапускаем DNS сервер :

```
# /etc/init.d/named restart
```

Теперь всем хостам в локальной сети можно указать этот сервер в качестве DNS сервера.

Проверить работоспособность можно следующим образом:

```
$ nslookup -sil www.linux.org
Server:         222.222.222.222
Address:        222.222.222.222#53

Non-authoritative answer:
Name:   www.linux.org
Address: 198.182.196.56

$ nslookup -sil www.linux.org
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
Name:   www.linux.org
Address: 198.182.196.56
```

Как мы видим, первый раз обращение прошло к DNS серверу вашего провайдера, а второй раз ответ получен из кеша вашего DNS сервера.

3.2. Настройка первичного(master) DNS сервере и создание прямой и обратной зоны.

Допустим у Вас есть доменное имя mynet.lan Вам хочется сделать свой сервер первичным сервером для этого домена и использовать у себя в сети доменные имена www.mynet.lan, kolya.mynet.lan и т.д. Для этого сначала попрвим файл `/etc/named.conf`

```
//////////////////////////////////////////////////////
key mykey {
       algorithm hmac-md5;
       secret "IriCelUSbPMypSjImBsiTHMauOumRPMkdBjoxVINAx0vxJZNRKGWzFCKibad";

};
controls {
    inet 127.0.0.1   allow { any; } keys { "mykey"; };

    // эту строка добавлена здесь для целей которые описанны в главе про DHCP
    inet 192.168.1.4 allow { any; } keys { "mykey"; };


};
options {
 pid-file "/var/run/named/named.pid";
 directory "/var/named";
 /*
  * If there is a firewall between you and nameservers you want
  * to talk to, you might need to uncomment the query-source
  * directive below.  Previous versions of BIND always asked
  * questions using port 53, but BIND 8.1 uses an unprivileged
  * port by default.
  */
 // query-source address * port 53;
 // здесь вместо 222.222.222.222 проставте ip DNS сервера вашего провайдера
 forwarders { 127.0.0.1; 222.222.222.222; };
 forward first;
};

//
// a caching only nameserver config
//
zone "." {
 type hint;
 file "named.ca";
};
zone "0.0.127.in-addr.arpa" {
 type master;
 file "named.local";
};

// Прямая и обратные зоны для домена mynet.lan

zone "mynet.lan" {
        type master;
        file "mynet.zone";
        allow-update { key mykey; };
};

zone "1.168.192.in-addr.arpa" {
        type master;
        file "mynet.reversed";
        allow-update { key mykey; };
};
//////////////////////////////////////////////////////
```

Как мы видим в конце файла добавилены две записи "zone". Теперь нам необходимо создать еще 2 файла содержащих прямую и обратную зону.

Создаем файл обратной зоны `/var/named/mynet.reversed`.

```
$ORIGIN .
$TTL 86400 ; 1 day
```

```
1.168.192.in-addr.arpa IN SOA ns.mynet.lan. ns.mynet.lan. (
    2001042703 ; serial
    28800      ; refresh (8 hours)
    14400      ; retry (4 hours)
    3600000    ; expire (5 weeks 6 days 16 hours)
    86400      ; minimum (1 day)
    )
   NS ns.mynet.lan.
$ORIGIN 1.168.192.in-addr.arpa.
$TTL 3600 ; 1 hour
1   PTR router.mynet.lan.
4   PTR ns.mynet.lan.
```

теперь создаем файл прямой зоны `/var/named/mynet.zone`

```
$ORIGIN .
$TTL 86400 ; 1 day
mynet.lan  IN SOA ns.mynet.lan. ns.mynet.lan. (
    2001042705 ; serial
    86400      ; refresh (1 day)
    21600      ; retry (6 hours)
    3600000    ; expire (5 weeks 6 days 16 hours)
    3600       ; minimum (1 hour)
    )
   NS ns.mynet.lan.
$ORIGIN mynet.lan.
localhost  A 127.0.0.1
ns   A 192.168.1.4
router   A 192.168.1.1
www   A 192.168.1.1
```

По аналогии в конец файла прямой и обратной зон вы можете дописывать все что угодно. Обратите внимание на то что изменения вступают в силу только после изменения поля "serial". Обычно после внесения любых изменений в эти файлы serial увеличивают на 1.

3.3. Передача(forward) зоны

Иногда необходимо отдать какуюто часть домена для обслуживания другому DNS серверу. Это называется форвардинг зоны. Для этого можно просто добавить примерно такую запись в файл `/etc/named.conf`

```
zone "subnet.mynet.lan"{
      type forward first;
      forwarders {10.10.10.10;};
};
```

В этом примере subnet.mynet.lan - поддомен который вы передаете DNS серверу с IP 10.10.10.10. С этого момента обращения за доменными именами *.subnet.mynet.lan будут проходить не к вашеиу DNS серверу а к серверу 10.10.10.10

3.4. Настройка вторичного(secondary) DNS сервера

Иногда необходимо "просекондарить зону" - тоесть настроить свой DNS таким образом чтобы он был вторичным DNS сервером для какой либо зоны. По правилам необходимо чтобы у каждого первичного DNS сервера (master) было как минимум 2 вторичных (slave). Также это может быть необходимо если вам по какимто причинам нужно сделать свой сервер "авторитетным" для какой либо произвольной зоны. Просекондерить свой DNS можно двумя способами:

- С помощью web сервиса на http://secondary.net.ua/
- Настроить свой сервер самостоятельно добавив в файл `/etc/named.conf` примерно такую запись:

```
zone "subnet2.mynet.lan" {
        type slave;
        file "subnet2.mynet.lan.slave";
        masters { 10.10.10.10; };
};
```

В этом примере мы "секондарим" зону subnet2.mynet.lan первичным DNS сервером которой является сервер с IP 10.10.10.10 . после перезапуска DNS сервера должен создаться файл `/var/named/subnet2.mynet.lan.slave` в котором будет зона которую мы секондарим.

Глава 4. Настройка DHCP сервера

DHCP (Dynamic Host Configuration Protocol), динамический протокол настройки хостов - это протокол, который дает возможность компьютерам в сети получать свои сетевые настройки у сервера. В "сетевые настройки" входит IP-адрес, маска подсети, адрес DNS сервера, шлюз по умолчанию (default gateway). Также DHCP может взаимодействовать с DNS сервером и динамически менять в нем имена хостов. В GNU/Linux протокол DHCP поддерживается демоном dhcpd

4.1. Простейший DHCP сервер

Установим DHCP сервер:

```
# urpmi dhcp-server
```

Запуск DHCP сервера:

```
# /etc/init.d/dhcpd start
```

Останов DHCP сервера:

```
# /etc/init.d/dhcpd stop
```

После установки необходимо создать конфигурационный файл /etc/dhcpd.conf. Можно просто скопировать файл примера:

```
cp /etc/dhcpd.conf.sample /etc/dhcpd.conf
```

Далее мы будем вносить изменения в этот конфигурационный файл /etc/dhcpd.conf.

Рассмотрим самый простейший вариант использования DHCP сервера: пусть мы хотим, чтобы все хосты в сети 192.168.1.0/24 получали IP в диапазоне 192.168.1.128-250. Также нам нужно, чтобы машины в сети использовали по умолчанию шлюз 192.168.1.1 и DNS сервер 192.168.1.4. Кроме того нам нужно чтобы клиентская машина знала что она работает в домене mynet.lan.

Настройки такого сервера выглядят следующим образом:

```
ddns-update-style none;
subnet 192.168.1.0 netmask 255.255.255.0
{
    option routers 192.168.1.1;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 192.168.1.4;
    option domain-name "mynet.lan";

    range 192.168.1.128 192.168.1.250;
}
```

В нашем примере первая, обратившаяся за настройками, машина получит адрес 192.168.1.250, следующая 192.168.1.249 ну и так далее.

В случае, если нам нужно, чтобы некоторые компьютеры в сети получали вместо случайных адресов только жестко закрепленный за ними адрес (в соответствии с аппаратным MAC-адресом сетевой карты), тогда можно использовать такую конфигурацию:

```
ddns-update-style none;
subnet 192.168.1.0 netmask 255.255.255.0
{
    option routers 192.168.1.1;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 192.168.1.4;

    range 192.168.1.128 192.168.1.250;

    host smith # Вася Сидоров :-)
    {
        hardware ethernet 00:0c:29:8b:02:e7;
        fixed-address 192.168.1.5;
    }
```

```
    host neo # Коля Петров
    {
        hardware ethernet 00:22:22:22:22:22;
        fixed-address 192.168.1.6;
    }
}
```

В этом примере IP-адреса раздаются с привязкой к MAC-адресу сетевой карты. Сетевая карта с MAC `00:0c:29:8b:02:e7` всегда будет получать адрес `192.168.1.5`, а сетевая карта с MAC `00:22:22:22:22:22` соответственно адрес `192.168.1.6`, а остальные компьютеры в сети будут получать адреса случайным образом в диапазоне с `192.168.1.128` по `192.168.1.250`. Если мы хотим чтобы IP-адреса получали только компьютеры, привязанные к MAC, тогда в данном примере нужно закомментировать строку `range 192.168.1.128 192.168.1.250;`.

4.2. Настройка динамического DHCP сервера, связанного с DNS

Работает это следующим образом: машина в сети получает случайный IP-адрес и, при получении этого IP, DHCP сервер перенастраивает DNS сервер таким образом, чтобы у компьютеров в сети независимо от того, какой у них в данный момент IP, всегда было одно и тоже доменное имя.

Файлы `/etc/named.conf`, `/var/named/mynet.reversed`, `/var/named/mynet.zone` должны выглядеть точно так, как было описано здесь: Гл. 3.

Теперь приведем как должен выглядеть файл `/etc/dhcpd.conf`:

```
### begin of /etc/dhcpd.conf ######################################################
ddns-update-style ad-hoc;

subnet 192.168.1.0 netmask 255.255.255.0
{
    option routers 192.168.1.1;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 192.168.1.4;

    range 192.168.1.5 192.168.1.250;

    ddns-updates on;
    ddns-domainname "mynet.lan";
    ddns-rev-domainname "in-addr.arpa";

    option domain-name "mynet.lan";

    # Этот "secret" нужно пересоздать с помощью команды dnssec-keygen
    # он должен быть ОДИНАКОВЫМ в этом файле, а также в
    # /etc/named.conf /etc/rndc.conf /etc/rnd.key
        key mykey {
 algorithm hmac-md5;
 secret "IriCelUSbPMypSjImBsiTHMauOumRPMkdBjoxVINAx0vxJZNRKGWzFCKibad";
    };

    zone mynet.lan. {
  primary 192.168.1.4;
  key mykey;
    }

    zone 1.168.192.in-addr.arpa. {
  primary 192.168.1.4;
  key mykey;
    }

    host smith # Агент Смит
    {
        hardware ethernet 00:0c:29:8b:02:e7;
# option host-name "vasya";
 ddns-hostname "smith";
    }

    host neo # Коля Петров
    {
```

```
        hardware ethernet 00:22:22:22:22:22;
# option host-name "kolya";
 ddns-hostname "neo";
    }
}
### end of /etc/dhcpd.conf ##################################################
```

В этом примере машина с MAC-адресом `00:0c:29:8b:02:e7` получит имя `smith.mynet.lan`, а машина с MAC-адресом `00:22:22:22:22:22` получит имя `neo.mynet.lan`. Имена остальных машин будут формироваться на основе запроса DHCP клиента. В случае с M$ Window$ это будет “имя компьютера”.

Для того, чтобы DHCP сервер мог управлять DNS сервером, необходимо также отредактировать следующие файлы: `/etc/rndc.conf`

```
###### begin of /etc/rndc.conf ##################
key mykey {
        algorithm hmac-md5;
        secret "IriCelUSbPMypSjImBsiTHMauOumRPMkdBjoxVINAx0vxJZNRKGWzFCKibad";
};

options {
        default-key mykey;
        default-server 127.0.0.1;
        default-port 953;
};
###### End of /etc/rndc.conf ####################
```

и `/etc/rndc.key`

```
key mykey {
       algorithm hmac-md5;
       secret "IriCelUSbPMypSjImBsiTHMauOumRPMkdBjoxVINAx0vxJZNRKGWzFCKibad";
};
```

После выполнения всех этих настроек перезапускаем DNS сервер и DHCP сервер и работаем.

Глава 5. Как раздать интернет на локальную сеть

Мы хотим, чтобы машины из локальной сети имели доступ к Internet. В данном случае наш сервер должен выполнять функции роутера (маршрутизатора). В нем должно быть как минимум два интерфейса:

- один подключен к интернет-провайдеру (пусть это eth0);
- а второй включен во внутреннюю сеть (пусть это eth1);

Для "раздачи" интернет во внутреннюю сеть часто используется IP маскарадинг (IPMASQUARADE). Работает это, вкратце, следующим образом: пакет, [1] поступающий из локальной сети на роутер, в своем заголовке содержит IP адрес создавшего его компьютера (далее ip-источника) и IP-адрес пункта назначения (далее ip-получателя). Роутер в этом случае подменяет ip-источника на свой ip и отправляет этот пакет получателю. Получатель формирует ответный пакет для роутера. Роутер принимает этот пакет, но он знает, что этот пакет предназначен не ему (путем запоминания номера пакета) и, заменяет в нем ip-получателя на ip-источника, затем отправляет этот пакет локальной машине в сети. Таким образом, получается, что машины во внутренней сети получают доступ в интернет от имени роутера. Отсюда и название "IP-маскарадинг", так как маршрутизатор маскирует своим IP машины внутри локальной сети. Это дает возможность серьезно повысить защищенность рабочих станций внутри сети и обеспечить их интернетом без раздачи им реальных IP адресов.

В отличии от прокси сервера (например SQUID), этот способ позволяет хорошо работать не только http, но и ftp/pop3/smtp/ssh/telnet/..... практически ЛЮБОМУ сервису. При этом не нужно объяснять сервису, что он работает через прокси.

Делается это одной командой:

```
# iptables -t net -A POSTROUTING -o <интерфейс, который наружу> -s <докальная сетка> -j MASQUERADE
```

Не забываем включить перенаправление пакетов:

```
# echo 1 >/proc/sys/net/ipv4/ip_forward
```

Полное описание того, что такое IP-Masquarade и как его настраивать на английском языке, можно получить здесь: http://www.ibiblio.org/pub/Linux/docs/HOWTO/other-formats/html/IP-Masquerade-HOWTO-html.tar.gz[2]. В частности, оттуда нас интересует раздел: 3.4.1. Выбираем оттуда первый примерчик (выделенный серым цветом), копируем его в файл и делаем этот файл запускаемым.

В адаптированном для Linux Mandrake 9.1-9.2 виде этот скрипт можно получить здесь: http://lafox.net/docs/masq/. Для других дистрибутивов, вероятно, нужно поправить пути в переменных : `IPTABLES`, `DEPMOD`, `MODPROBE`.

В сокращенном виде (без комментариев и нефункциональных выводов сообщений) скрипт выглядит так:

```
#!/bin/sh
# полная версия находится здесь: http://lafox.net/docs/masq/
IPTABLES=/sbin/iptables
DEPMOD=/sbin/depmod
MODPROBE=/sbin/modprobe

EXTIF="eth0"
INTIF="eth1"

$DEPMOD -a

$MODPROBE ip_tables
$MODPROBE ip_conntrack
$MODPROBE ip_conntrack_ftp
$MODPROBE ip_conntrack_irc
$MODPROBE iptable_nat
$MODPROBE ip_nat_ftp
$MODPROBE ip_nat_irc

echo "1" > /proc/sys/net/ipv4/ip_forward
```

1. IP пакет также часто называют datagram.
2. http://www.ibiblio.org/pub/Linux/docs/HOWTO/other-formats/html/IP-Masquerade-HOWTO-html.tar.gz

```
echo "1" > /proc/sys/net/ipv4/ip_dynaddr

$IPTABLES -P INPUT ACCEPT
$IPTABLES -F INPUT
$IPTABLES -P OUTPUT ACCEPT
$IPTABLES -F OUTPUT
$IPTABLES -P FORWARD DROP
$IPTABLES -F FORWARD
$IPTABLES -t nat -F

$IPTABLES -A FORWARD -i $EXTIF -o $INTIF -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPTABLES -A FORWARD -i $INTIF -o $EXTIF -j ACCEPT
$IPTABLES -A FORWARD -j LOG

$IPTABLES -t nat -A POSTROUTING -o $EXTIF -j MASQUERADE

echo -e "done.\n"
```

Давайте сохраним это в файлик и назовем его, к примеру `masq.sh`. Далее поправляем переменные:

```
EXTIF="eth0"
INTIF="eth1"
```

- EXTIF - это название интерфейса, который “смотрит” в сторону провайдера.
- INTIF - это название интерфейса, который “смотрит” во внутреннюю сеть.

Также, возможно, следует закомментировать строку:

```
$IPTABLES -A FORWARD -j LOG
```

Этим мы отключим логирование. Иначе, в больших сетях могут возникнуть проблемы с огромными размерами `log` файлов.

Далее просто запускаем этот скрипт и радуемся тому, что локальная сеть получила интернет. **:-)**

Посмотреть на то, что сделал этот скрипт с `iptables`, можно командочками:

```
# iptables -L
# iptables -L -t nat
```

IP-маскарадинг часто используется совместно с кэширующим прокси-сервером. О том, как его настроить читайте здесь: Гл. 6.

Глава 6. Настройка кэширующего прокси-сервера

Прокси-сервер в локальной сети - полезная штука для того, чтобы сэкономить http трафик. Его можно и нужно использовать совместно с IP-маскарадом.

Устанавливаем proxy сервер:

```
# urpmi squid
```

Затем ищем в файлике `/etc/squid/squid.conf` строку:

```
acl CONNECT method CONNECT
```

Вероятно это будет 1687-ая строка. После нее вставляем строку:

```
acl mynet src 192.168.1.0/255.255.255.0
```

где `192.168.1.0/255.255.255.0` - это ваша сеть, которая должна иметь право пользоваться этим прокси, а `mynet` это название правила. Правило может иметь другое имя, и их может быть несколько. В нашем примере мы будем его называть `mynet`.

> **Внимание**
>
> Не делайте здесь доступ из сетей вида `0/0` !!!! То есть не открывайте доступ всему интернету.

В конец файла дописываем `visible_hostname название.вашего.хоста`[1]

Теперь ищем строку:

```
http_access allow localhost
```

и после нее вставляем следующее:

```
http_access allow mynet
```

Затем перезапускаем прокси-сервер:

```
 # /etc/init.d/squid restart
```

Также может быть полезно добавить в конце файла конфигурации `/etc/squid/squid.conf` следующие строки:

- `maximum_object_size 1 GB`: максимальный размер кэшируемого объекта. Больше 1Гб не ставьте!
- `cache_mgr admin@your.domin.name`: email администратора прокси-сервера. Будет виден для пользователей при создании squid-ом страниц с отчетами об ошибках для пользователей.
- `cache_mem 64 MB`: размер оперативной памяти, который может использовать squid для своих нужд. Обратите внимание, что он может использовать на 10-20 % больше, чем здесь указано.
- `cache_dir ufs /var/spool/squid 5000 16 256`: самая интересная вещь: здесь устанавливается максимальное количество места на диске, которое может использовать squid для хранения кэшируемых объектов. В данном примере это 5Гб. (5000). 16 и 256 лучше оставить как есть. Если вы меняете цифру `5000` в конфиге, тогда нужно пересоздать кеш командой **# squid -z**, предварительно остановив squid. При этом старый кеш будет утерян.
- `#cache_peer XXX.XXX.XXX.XXX parent XX 3130`: полезная опция, если ваш провайдер предоставляет вам свой прокси-сервер. Этой строкой мы сообщаем нашему прокси-серверу, что он должен использовать прокси-сервер провайдера как ведущий, то есть посылать запросы не напрямую к сайтам, а через сервер провайдера с IP `XXX.XXX.XXX.XXX`, и порт `XX. 3130` - это ваш локальный порт, с которого будут устанавливаться соединения с прокси-сервером провайдера.

---

1. Установить эту переменную необходимо если для IP адреса вашего хоста не существует имени в зоне DNS наличие обратной зоны можно проверить командой **# host ваш.ip**

Замечание: С некоторыми прокси-серверами использование исходящего порта 3130 может не работать в этом случае рекомендуем использовать такую строку: `#cache_peer XXX.XXX.XXX.XXX parent XX 0 no-query`

Итак, у вас теперь есть кэширующий прокси-сервер для вашей сети. Заметим, что это, мягко выражаясь, очень поверхностное описание настройки squid, что возможно бросается в глаза при оценке размеров файла конфигурации этого сервера **:-)**. Тем не менее, этих действий обычно достаточно для небольших сетей.

Глава 7. Настройка FTP сервера

Проверяем что установлен или устанавливаем пакет ProFTPd

```
# urpmi proftpd
```

Файл конфигурации для FTP сервера ProFTPd это /etc/proftpd.conf. Все настройки и изменения мы будем делать именно в нем.

Запускаем сервер:

```
# /etc/init.d/proftpd restart
```

проверяем работоспособность

```
$ lftp admin@localhost
```

вводим пароль пользователя admin. Теперь выполняем команду **ls** и убеждаемся, что мы находимся в домашнем каталоге пользователя admin. Выполняем команду **cd /** и **ls** и убеждаемся, что FTP сервер пустил нас выше домашнего каталога пользователя, что часто НЕЖЕЛАТЕЛЬНО. Выходим из FTP клиента (команда **quit**).

Чтобы этому воспрепятствовать, пишем в файле конфигурации строчечку DefaultRoot ~. Это значит, что мы "запираем" всех пользователей в их домашних каталогах. А если нам все-таки хочется пустить какого-то пользователя (пусть это будет testuser) выше, добавляем еще одну строку DefaultRoot / testuser.

Часто используется анонимный FTP сервер (anonymous ftp). Настроить его легко можно так: добавьте следующий код в конец конфигурационного файла /etc/proftpd.conf (каталог /var/ftp/ по умолчанию является каталогом, где лежат общедоступные файлы и домашним каталогом пользователя ftp, под которым запускается демон ProFTPd):

```
##########################################
<Anonymous /var/ftp/>
  User    ftp
  Group    ftp

  # Рассматривать клиентов, вошедших под логином anonymous как ftp
  UserAlias   anonymous ftp

  # Лимит на максимальное количество подключений пользователя anonymous
  MaxClients   30

  # не спрашивать пароля и оболочку.
  RequireValidShell  off
  AnonRequirePassword  off

  # ограничение ЗАПИСИ(WRITE) везде в anonymous chroot
  <Limit WRITE>
    Order Deny, Allow
    DenyAll
  </Limit>

</Anonymous>
##########################################
```

Теперь перезапускаем ProFTPd сервер и проверяем, что анонимный доступ на FTP работает:

```
$ links ftp://localhost/
```

Часто используется анонимный FTP сервер, который предоставляет возможность пользователям загружать файлы на сервер. Для того, чтобы это сделать, сначала необходимо создать каталог внутри корня анонимного FTP сервера, в который эти пользователи будут иметь доступ, и сделать его владельцем пользователя ftp.

```
# mkdir /var/ftp/uploads
# chown ftp.ftp /var/ftp/uploads
```

Теперь добавим следующий код конфигурационный файл `/etc/proftpd.conf` внутрь секции <anonymous> (например перед ее закрытием, то есть перед строкой </anonymous>):

```
    <Directory uploads/*>
       <Limit READ>
           DenyAll
       </Limit>
        <Limit STOR>
            AllowAll
        </Limit>
    </Directory>
```

Теперь в каталог `/var/ftp/uploads` пользователи могут заливать файлы, используя анонимную авторизацию. При этом файлы в этом каталоге никто не сможет читать. Если вам захочется, чтобы загруженные в этот каталог файлы были доступны для чтения анонимным пользователям, тогда просто закомментируйте (или удалите) следующие строки:

```
#       <Limit READ>
#           DenyAll
#       </Limit>
```

Минимальные настройки FTP сервера закончены. Более расширенные инструкции поищите у себя в каталоге `/usr/share/doc/proftpd-1.2.7/`, а также на сайте разработчиков этого демона http://proftpd.org/

Глава 8. Настройка файлового сервера samba - совместимого с файловым сервером Windows

Samba - это файловый сервер, совместимый с файловым сервером M$ Window$. Его полезно и удобно использовать в сети, где есть машины под управлением M$ Window$.

Установка сервера:

```
# urpmi samba
```

Запуск сервера:

```
# /etc/init.d/smb start
```

Пример конфига /etc/samba/smb.conf, в котором ресурсы распределяются на уровне ресурсов:

```
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
[global]
 log file = /var/log/samba/log.%m
 guest account = ftp
 smb passwd file = /etc/samba/smbpasswd
 client code page = 866
 character set = KOI8-R
 hosts allow = 192.168.1. 127.
 encrypt passwords = yes
 dns proxy = no
 netbios name = SAMBA file server
 server string = Samba File Server %v
 default = ftp
 workgroup = MDK
 max log size = 500
 log level = 3
 load printers = no

 security = share

[ftp] ; Это работает аналогично анонимному FTP серверу
 guest account = nobody
 comment = anonymous share
 hide dot files = no
 map hidden = yes
 printable = no
 path = /var/ftp
 public = yes
 guest only = yes

[home-admin] ; Это предоставляет доступ юзеру admin(под паролем) в свой домашний каталог
 comment = admin Home Dir
 writable = yes
 valid users = admin
 path = /home/admin

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
```

Пример конфига /etc/samba/smb.conf, в котором ресурсы распределяются на уровне пользователей:

```
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
[global]
 log file = /var/log/samba/log.%m
 smb passwd file = /etc/samba/smbpasswd
 client code page = 866
 character set = KOI8-R
 hosts allow = 192.168.1. 127.
 encrypt passwords = yes
 dns proxy = no
 netbios name = SAMBA file server
 server string = Samba File Server %v
```

```
 workgroup = MDK
 max log size = 500
 log level = 3
 load printers = no

 security = users

[homes]; Это дает возможность всем пользователям получать доступ к своим домашним каталогам
    comment = Home directories
    browseable = yes
    writable = yes
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
```

Нужно добавить, что все пользователи, которые получают доступ через `Samba` должны быть:

1. Добавлены в систему (**#userconf --text**, **userdrake**, или **adduser/passwd**)
2. Добавлены как пользователи samba в `/etc/samba/smbpasswd`. Это нужно сделать командочкой **# smbpasswd -a admin**. Понятно, что вместо `admin` может фигурировать любой пользователь.

Проверяем работу, предварительно перезапустив `SMB` после редактирования конфига:

```
# mkdir /mnt/smb
# mount -t smbfs -o username=admin,password=ПАРОЛЬ,codepage=cp866,iocharset=koi8-r //127.0.0.1/home-
```

Разумеется, что вместо слова `ПАРОЛЬ` нужно подставить пароль пользователя `admin`. Путь `//127.0.0.1/home-admin` это стандартное для M$ Window$ описание разделяемых ресурсов (только все “\” заменяются на “/”).

Отмонтировать это можно командой:

```
# umount /mnt/smb
```

Более наглядно путешествовать по ресурсам M$ Window$ или `Samba` можно с помощью программы с графическим интерфейсом `LinNeighborhood` - весьма хорошая программа.

Глава 9. Настройка почты

Почтовый сервер может выполнять 3 независящие друг от друга функции:

- Отправлять почту от пользователей на другие SMTP сервера. (SMTP это `Send Mail Transport Protocol`). Этим занимается `Postfix`.
- Принимать почту по SMTP от других почтовых серверов и раскладывать ее по почтовым ящикам пользователей. Этим тоже занимается `Postfix`
- Предоставлять возможность пользователям с помощью почтовых клиентов забирать свою почту по протоколам POP3 или IMAP. Этим `Postfix` уже не занимается **:-)**.

Начнем с `Postfix`.

9.1. Установка/настройка почтового сервера postfix

Проверяем установлен ли пакет, содержащий почтовый сервер `Postfix`:

```
# urpmi postfix
```

Для запуска сервера выполняем команду:

```
# /etc/init.d/postfix start
```

Для останова сервера выполняем команду:

```
# /etc/init.d/postfix stop
```

Почтовый сервер `Postfix` сразу после установки имеет настройки, позволяющие использовать его как SMTP-сервер для отправки почты с локальной машины.

Тем не менее, мы рекомендуем изменить в конфигурационном файле `/etc/postfix/main.cf` следующие переменные:

- `myhostname = virtual.domain.tld` укажите здесь реальное имя вашего хоста (например, `mail.mycompanyname.com`
- `mydomain =domain.tld`: Укажите здесь ваше правильное почтовое доменное имя (например, `mycompanyname.com.ua`

Для того, чтобы предоставить возможность отправлять почту через этот SMTP другим хостам в вашей локальной сети, нужно в конфигурационном файле `/etc/postfix/main.cf` правильно определить следующие переменные:

- `inet_interfaces = all`: это необходимо сделать для того, чтобы к серверу могли подключаться не только локальные почтовые клиенты.
- Также необходимо поправить переменную `mynetworks`. Ее можно заменить к примеру на: `mynetworks = 127.0.0.0/8, 192.168.1.0/24` , где `192.168.1.0/24` это ваша подсеть, с которой вы разрешаете отсылать почту через этот SMTP сервер.

> **Внимание**
>
> Не открывайте доступ со всего мира! За такими открытыми серверами охотятся спамеры и используют такие сервера для рассылки спама. Кроме того, в этом случае можно также попасть в black-list.

Для того, чтобы ваш почтовый сервер мог принимать почту для вашего почтового домена, необходимо чтобы выполнялись следующие условия:

1. Должно быть настроено все что описано выше.
2. У вас должен быть статический IP-адрес и постоянное подключение к Интернет.

3. У вас должно быть зарегистрировано соответствующее доменное имя (например example.com).
4. Запись MX вашего домена должна указывать на данный хост.

Не забываем после внесения любых изменений в конфиги перезапускать `Postfix`, так как изменения вступают в силу только после перезапуска этого демона.

Добавим, что логи почтового сервера находятся в каталоге `/var/log/mail/`. Для просмотра в реальном режиме времени логов почтового сервера можно воспользоваться командой:

```
# tail -f /var/log/mail/info
```

Кроме того, часто бывает полезно посмотреть на очередь сообщений сервера. Это можно сделать командочкой:

```
# mailq
```

Если вы хотите форсировать отправку писем из очереди, этого можно добиться командой:

```
# postfix flush
```

9.2. Установка pop3/imap сервера

Допустим, прочитав предыдущую часть, вы успешно настроили почтовый сервер таким образом, что он может отправлять и принимать почту. Теперь нужно добиться того, чтобы пользователи могли забирать свою почту с сервера. Для этого обычно используется протокол POP3 (`Post Office Protocol version 3`) или, реже, протокол IMAP. Можно также использовать защищенные версии этих протоколов POP3s и IMAPs.

Устанавливаем пакет imap:

```
# urpmi imap
```

Этот пакет содержит сервисы, позволяющие использовать любой из четырех вышеописанных протоколов. Теперь нам осталось только включить необходимые нам сервисы.

Итак, мы имеем дело со следующими демонами: `ipop3`, `pop3s`, `imap`, `imaps`. Запуском этих демонов занимается демон `xinetd`. Для примера мы рассмотрим как включить демон ipop3, как самый широко используемый. Аналогичные действия можно и нужно провести со всеми четырьмя демонами.

Узнаем состояние демона, то есть определяем включен ли он в `xinetd`:

```
# chkconfig --list ipop3
```

Если не включен, включаем демон в `xinetd`:

```
# chkconfig ipop3 on
```

Отключить демон в `xinetd` можно так:

```
# chkconfig ipop3 off
```

Обратите внимание, что опция `on` сразу загружает это сервис и делает его активным, а опция `off` сразу выключает и выгружает этот сервис.

Никакой дополнительной настройки эти сервисы обычно не требуют.

Глава 10. Настройка WWW сервера apache

10.1. Установка и простейшая настройка

Инсталляция :

```
# urpmi apache
```

Запуск сервера:

```
# apachectl start
```

Останов сервера:

```
# apachectl stop
```

Перезапуск сервера :

```
# apachectl restart
```

Проверка работоспособности сервера:

```
# links http://localhost/
# echo "<?phpinfo()?>">/var/www/html/phpinfo.php
# links http://localhost/phpinfo.php
```

Кстати, двумя последними строками вы также проверите работоспособность PHP.

Для того, чтобы правильно отображались русскоязычные документы, в файле `/etc/httpd/conf/commonhttpd.conf` нужно изменить строчку : `AddDefaultCharset ISO-8859-1` на `AddDefaultCharset KOI8-R` или на `AddDefaultCharset CP1251`. Если в теге <META> ваших html документов уже прописана нужная кодировка, тогда вам может подойти вариант `AddDefaultCharset off`.

В файле `/etc/httpd/conf/httpd2.conf` можно изменить: Переменную `DocumentRoot /var/www/html` Это место, где находится корень ваших html-документов, публикуемых в сети. Также очень полезно определить переменную `ServerName имя_вашего_домена`.

Сервер полностью готов к работе. Подробнее, какие еще опции полезно настраивать, смотрите ниже в разделе про виртуальные хосты.

10.2. Настройка виртуальных хостов

Теперь мы рассмотрим настройку виртуальных хостов. Допустим, у вас есть IP-адрес xxx.xxx.xxx.xxx и следующие доменные имена: `host1.aa`, `www.host1.aa`, а также `host2.aa`, `www.host2.aa`, которые указывают на IP-адрес `xxx.xxx.xxx.xxx`.

Задача состоит в следующем: нам нужно, чтобы на два первых домена (`host1.aa` и `www.host1.aa`) отзывался web-сайт, файлы которого находятся в каталоге `/var/www/www.host1.aa/WebRoot`, а на два других (`host2.aa` и `www.host2.aa`) отзывался web-сайт, файлы которого находятся в каталоге `/var/www/www.host2.aa/WebRoot`. Также нужно, чтобы работал PHP. Кроме того, web-сайт по адресу `www.host2.aa` должен быть доступен только из нашей внутренней сети (так как это внутренний сайт для корпоративного пользования), а вот сайт `www.host1.aa` должен быть доступен также и из внешнего мира.

Для этого мы сделаем следующее: в файл `/etc/httpd/conf/vhosts/Vhosts.conf` добавляем следующие строки:

```
NameVirtualHost xxx.xxx.xxx.xxx:80

<VirtualHost xxx.xxx.xxx.xxx:80>
    ServerAdmin     admin@host1.aa
    DocumentRoot    /var/www/www.host1.aa/WebRoot
    ServerName      www.host1.aa
    ServerAlias     host1.aa
    AddType         application/x-httpd-php .php
    ErrorLog        /var/log/httpd/host1.aa-error_log
    CustomLog       /var/log/httpd/host1.aa-access_log combined
    DirectoryIndex  index.html index.php index.htm
```

```
    AddDefaultCharset KOI8-R
</VirtualHost>
<Directory  /var/www/www.host1.aa>
<IfModule mod_php4.c>
    php_admin_value safe_mode on
    php_admin_value allow_url_fopen off
    php_admin_value max_execution_time 30
    php_admin_value open_base_dir /var/www/www.host1.aa/
    php_admin_value memory_limit  2M
    php_admin_value default_charset KOI8-R
</IfModule>
    AllowOverride  None

    Options FollowSymlinks

    Allow from all

</Directory>

##########################################
<VirtualHost xxx.xxx.xxx.xxx:80>
    ServerAdmin     admin@host2.aa
    DocumentRoot    /var/www/www.host2.aa/WebRoot
    ServerName      www.host2.aa
    ServerAlias     host2.aa
    AddType         application/x-httpd-php .php
    ErrorLog        /var/log/httpd/host2.aa-error_log
    CustomLog       /var/log/httpd/host2.aa-access_log combined
    DirectoryIndex  index.html index.php index.htm
    AddDefaultCharset KOI8-R
</VirtualHost>
<Directory  /var/www/www.host2.aa>
<IfModule mod_php4.c>
    php_admin_value safe_mode on
    php_admin_value allow_url_fopen off
    php_admin_value max_execution_time 30
    php_admin_value open_base_dir /var/www/www.host2.aa/
    php_admin_value memory_limit  2M
    php_admin_value default_charset KOI8-R
</IfModule>
    AllowOverride  None

    Options FollowSymlinks

    Order Deny,Allow
    Deny from all
    Allow from  192.168.1.0/24

    #Allow from all

</Directory>
```

Поясним ниже опции, которые мы использовали в нашем примере настройки:

- `ServerAdmin admin@host2.aa` : эта опция определяет email-адрес, который будет появляться в сообщении при ошибках сервера. Иначе говоря, сервер будет предлагать обращаться администратору сервера по этому адресу.
- `DocumentRoot /var/www/www.host1.aa/WebRoot`: этим мы определяем корневой каталог для веб-сервера, где лежат на диске файлы вашего сайта.
- `ServerName www.host2.aa`: здесь мы указываем имя виртуального хоста, на которое сервер должен отзываться, когда его набирают в браузере.
- `ServerAlias host2.aa`: это псевдоним ServerName. Этим мы объясняем, что под именами `www.host2.aa` и `host2.aa` будет появляться один и тот же сайт. Таким образом можно перечислить все доменные имена, если их несколько, на которые будет отзываться данный виртуальный хост. Все эти доменные имена должны иметь соответствующую запись в DNS.

- `AddType application/x-httpd-php .php`: эта опция включает интерпретатор `PHP` для документов с расширением `.php`.
- `ErrorLog /var/log/httpd/host2.aa-error_log`: в этот файл пишется журнал ошибок сервера.
- `CustomLog /var/log/httpd/host2.aa-access_log combined`: в этот файл пишется журнал о посещениях вашего сайта. `combined` означает подробный лог. Если мало места на диске, можно использовать простой лог `common`.
- `DirectoryIndex index.html index.php index.htm`: этим мы говорим, что индексными файлами каталогов будут файлы с именами `index.html`, `index.php`, `index.htm`.
- `AddDefaultCharset KOI8-R`: этим мы заставляем сервер слать в `http` заголовке кодировку `KOI8-R`. Если это не указывать, сервер шлет по умолчанию `ISO-8859-1`. Чтобы `Apache` вообще ничего не слал в заголовке, поставьте `AddDefaultCharset off`. В таком варианте браузер будет руководствоваться тем, что написано в <META> ваших html документов.
- `php_admin_value safe_mode on`: эта опция заставляет `PHP` работать в безопасном режиме. Это значит, что блокируются некоторые опасные функции `PHP`.
- `php_admin_value allow_url_fopen off`: этим мы запрещаем `PHP` открывать соединения с внешними серверами с помощью функций `fopen()`, `file()` и т.д.. То есть блокируем такие действия, как `<? $content=file('http://lafox.net/');?>`.
- `php_admin_value max_execution_time 30`: этим мы указываем, что скрипт `PHP` нужно обрывать после 30 секунд работы. Эта опция важна для предотвращения зацикливаний, а так же снижает опасность "DoS" атак на сервер (атак на отказ в обслуживании).
- `php_admin_value open_base_dir /var/www/www.host2.aa/`: этим мы запрещаем всем функциям `PHP` доступ к файлам, находящимся выше каталога `/var/www/www.host2.aa/`. Этот запрет не дает возможность вашим пользователям выполнять такие вредоносные операции, как `<? $content=file('/etc/password');?>` что значительно увеличивает защиту сервера от атак и ошибок при программировании `PHP`-скриптов.
- `php_admin_value memory_limit 2M`: этим мы ограничиваем размер памяти, который может использовать `PHP`-скрипт. Это важный параметр, так как он предотвращает перегрузку сервера из-за ошибок в скриптах, вызывающих неограниченное использование памяти. Так же этим мы уменьшаем опасность "DoS" атак.
- `php_admin_value default_charset KOI8-R`: это заставляет `PHP` посылать в `HTTP` заголовке информацию о кодировке данных. Обратите внимание, что опция `AddDefaultCharset`, описанная выше, не действует на `PHP` скрипты.
- `AllowOverride None`: опция запрещает перекрывать настройки общего конфиг-файла файлом `.htaccess`. Если вы хотите оставить эту возможность, напишите `AllowOverride all`.
- `Options FollowSymlinks`: разрешает использование символических ссылок.
- `Order Deny,Allow`: определяет порядок применения правил по запрещению и предоставлению доступа.
- `Deny from all`: запрещает доступ к этому виртуальному хосту отовсюду.
- `Allow from 192.168.1.0/24`: эта опция разрешает доступ к сайту из сети `192.168.1.0/24`.
- `Allow from all`: разрешает доступ к нашему виртуальному хосту отовсюду.

Для установки CGI версии php (это, например, полезно в случае, если нужно выполнять скрипты на php в командной оболочке), устанавливаем

```
# urpmi php-cgi
```

10.3. Ограничение доступа

Допустим, нам необходимо ограничить доступ в определенный каталог web-сервера по адресу, например `http://www.host2.aa/private/`. Мы хотим, чтобы туда могли попасть только пользователи из сети `10.10.11.0/24`. Этот web-адрес в нашем случае соответствует физическому каталогу на диске `/var/www/www.host2.aa/WebRoot/private/`. Тогда нам нужно добавить в конфиг-файл такой блок:

```
<Directory  /var/www/www.host2.aa/WebRoot/private>
```

```
    Order Deny,Allow
    Deny from all
    Allow from    10.10.11.0/24
</Directory>
```

Теперь, допустим, нам нужно чтобы при входе на web-адрес `http://www.host2.aa/admin/`, что соответствует физическому каталогу на диске `/var/www/www.host2.aa/WebRoot/admin`, сервер запрашивал логин и пароль и пропускал туда только пользователей `admin` и `manager` с паролями `adminpass` и `manpass` соответственно. Тогда сначала добавляем в конфигурационный файл такой блок:

```
<Directory  /var/www/www.host2.aa/WebRoot/admin>
    AuthName "ADMINSTRATOR AREA"
    AuthType basic
    AuthUserFile "/var/www/www.host2.aa/.htpasswd"
    Require valid-user
    Allow from All
</Directory>
```

Затем создаем файл с логинами и паролями `/var/www/www.host2.aa/.htpasswd`. Для этого выполняем следующую команду:

```
htpasswd -c /var/www/www.host2.aa/.htpasswd admin
```

и вводим дважды пароль. Ключик `-c` говорит о том, что мы создаем новый файл паролей. Соответственно, при добавлении новых пользователей этот ключик использовать нельзя. Теперь добавим второго пользователя:

```
htpasswd /var/www/www.host2.aa/.htpasswd manager
```

По запросу дважды вводим пароль (в нашем примере manpass). Перегружаем сервер и проверяем, что теперь при входе на `http://www.host2.aa/admin/`, сервер запросит логин и пароль.

> **Замечание:** Внимание: важно, чтобы файл `/var/www/www.host2.aa/.htpasswd` имел права на чтение для пользователя apache.

Глава 11. Настройка MySQL

В некоторых случаях необходимо установить SQL сервер MySQL. Сделать это несложно:

```
# urpmi mysql
```

Будет установлен как сервер, так и клиент.

Остановка сервера :**# /etc/init.d/mysql stop**; Запуск сервера:**# /etc/init.d/mysql start**. Проверить состояние сервера можно командой **mysqladmin -uroot status** .

Давайте создадим новую базу данных (например `mydb`), создадим пользователя (например `mydbadmin`) и настроим ему права, при которых он будет иметь доступ к этой базе. Пароль для доступа пусть будет `MyPas`

Создаем базу данных `mydb` так: **# mysqladmin -u root create mydb**. Затем добавляем пользователя `mydbadmin` с паролем `MyPas`. При этом разрешаем ему доступ к его базе данных только с `localhost`:

Теперь выдаем пользователю `mydbadmin` полные права для базы `mydb`. При этом пользователь `mydbadmin` по-прежнему ничего не может сделать с другими базами данных:

```
#mysql -uroot  mysql -e \
"GRANT ALL PRIVILEGES ON mydb.* TO mydbadmin@localhost  IDENTIFIED BY 'MyPass' WITH GRANT OPTION;"
```

После этого перезапускаем SQL сервер для того, чтобы изменения вошли в силу: **#mysqladmin -uroot reload**

Итог: сервер установлен, в нем создана новая база данных и заведен пользователь, имеющий полные права для работы с этой базой данных. Теперь давайте сделаем простейшие операции с базой (просто для разминки **:-)**).

Создаем пробную таблицу `test`:

```
# mysql -umydbadmin -pMyPas mydb -e "create table test(id int,name char(255));"
```

Вставляем в созданную таблицу 2-е записи:

```
# mysql -umydbadmin -pMyPas mydb -e \
"insert into test values('1','name1');insert into test values(2,'name2');"
```

Выбираем все записи из нашей таблички `test`:

```
# mysql -umydbadmin -pMyPas mydb -e "select * from test"
+------+-------+
| id   | name  |
+------+-------+
|    1 | name1 |
|    2 | name2 |
+------+-------+
```

Убиваем созданную нами табличку `test`:

```
# mysql -umydbadmin -pMyPas mydb -e "drop table test"
```

Как мы видим, сервер работает нормально.

Не забудьте добавить демона `mysqld` в автозагрузку:

```
# chkconfig mysqld on
```

Глава 12. Приложения для работы на каждый день

В этой главе мы расскажем о том, какие приложения можно использовать в Linux для решения повседневных задач, для которых используется рабочая станция. Глава в основном предназначена для быстрой адаптации в среде Linux. .

12.1. Почта и Интернет

12.1.1. Браузеры

В 3-х дисковый комплект поставки входят следующие браузеры:

- `Mozilla`[1] : прекрасный браузер с открытым исходным кодом.
- `Konqueror`[2] : немного облегченный браузер, интегрированный в `KDE`. Также выполняет функции файлового менеджера `KDE` (напоминает "проводник" в M$ Window$).
- galeon[3] : браузер среды `GNOME`, основанный на ядре проекта `Mozilla`. Введены некоторые усовершенствования интерфейса.

Также входят браузеры, работающие в текстовом режиме:

- lynx[4] : простейший из браузеров, но иногда полезный хотя бы для тестирования.
- links[5] : довольно продвинутый текстовый браузер, умеющий делать почти все, что делают браузеры с графической оболочкой.

Кроме того, существуют коммерческие браузеры:

- `Opera`[6]: на данный момент истории наверное самый лучший из браузеров. Легкий и многофункциональный. Его всегда можно скачать с сайта производителя http://www.opera.com.

12.1.2. Почтовые клиенты

Почтовые клиенты с графической оболочкой

- `kmail`[8]: отличный почтовый клиент, интегрированный в `KDE`. Чем-то напоминает `TheBat`. Имеет встроенную адресную книгу, может просматривать письма как в текстовом формате, так и в html. Прекрасно работает с такими системами защиты информации, как GnuPG.
- `Evolution`[9]: тоже замечательный почтовый клиент и органайзер. Чем-то напоминает Micro$oft Exchange.

Также есть встроенные почтовые клиенты в браузерах `Mozilla` и `Opera`. Существует еще несколько менее распространенных клиентов.

В Linux существуют также консольные (текстовые) почтовые клиенты:

- mutt[10]: который входит в стандартную поставку.

1. http://www.mozilla.org
2. http://www.konqueror.org
3. http://galeon.sourceforge.net/
4. http://lynx.browser.org/
5. http://links.sourceforge.net/
6. http://www.opera.com
8. http://kmail.kde.org/
9. http://www.ximian.com/products/evolution/
10. http://www.mutt.org/

- pine[11] мощный почтовый и news клиент, который почему-то в поставку не вошел.

Нужно также упомянуть, что в командной строке существует стандартная для UNIX утилита mail.

12.1.3. Чаты и общение

Начнем с IRC клиентов :

- `XChat`[12] : мощнейший IRC клиент. Имеет очень удобный графический интерфейс и массу удобных функций. Легко настраивается. `XChat` можно также использовать в консольном варианте.
- ksirc[13] : несколько упрощенный IRC клиент, входящий в состав `KDE`.
- BitchX[14] : очень мощный консольный IRC клиент.

Кроме того, браузер `Mozilla` имеет свой простенький встроенный IRC клиент.

Теперь об ICQ :

- licq[15] : полнофункциональный ICQ клиент с графическим интерфейсом.
- centericq[16]: это консольный ICQ клиент, совместимый с `ICQ2000`. Также может работать как клиент Yahoo!, MSN, AIM и IRC. Вообщем все в одной коробке.
- mICQ[17]: это текстовый клон “Mirabilis ICQ”.

ICQ клиенты `centericq` и `micq` не входят в основные 3 диска дистрибутива, но обычно присутствуют на “contribs CD”.

12.1.4. Качалки и FTP клиенты

Все браузеры, описанные в разделе о браузерах выше, вполне хорошо работают как FTP клиенты. Кроме того, существует стандартная для UNIX утилита `ftp`. Очень расширенная версия консольной утилиты `ftp` это `lftp`. Имеет режимы докачки, зеркалирования, пакетного выполнения команд и так далее. Также существует известная качалка **wget**, которая работает как с FTP, так и HTTP.

Отдельно можно вынести файловый менеджер `MidNight Commander`, который имеет встроенные ftp и sftp клиенты.

Также поставляется множество утилит с графическим интерфейсом:

- kget[18]: встроенный в `KDE` менеджер закачек. Довольно простой, но для большинства нужд вполне достаточен.
- gftp[19]: довольно мощный ftp/ftps клиент с графическим интерфейсом. Его достаточно практически на все случаи жизни.

Есть еще несколько хороших графических утилит для работы с FTP, которые не вошли в основные диски дистрибутива, но зато присутствуют в наборах “contrib”

- kbear[20]: многофункциональный ftp клиент с огромным количеством функций и возможностей. Может перекачивать файлы с одного сервера на другой мимо клиентской машины, делать перекодировки имен файлов из одной кодовой таблицы в другую и тд. `kbear` имеет современный и удобный графический пользовательский интерфейс. Это наверное самый мощный ftp клиент на данный момент. Имеет русский интерфейс пользователя.

11. http://www.washington.edu/pine/
12. http://xchat.org/
13. http://www.kde.org/
14. http://www.bitchx.org/
15. http://licq.org/
16. http://konst.org.ua/centericq/
17. http://www.micq.org/
18. http://kde.org/
19. http://www.gftp.org
20. http://kbear.sourceforge.net/

- nt[21] (Downloader for X): это программа является "калькой" с известного под M$ Window$ download менеджера `ReGet`. Работает как с FTP так и с HTTP. Имеет примерно такой же внешний вид и примерно такую же функциональность, как и `reget`. В дополнение, с ним можно работать без графического интерфейса, то есть с командной строки (примерно также, как с **wget**). Имеет русский интерфейс пользователя.

12.2. Офисные пакеты

Для выполнения обычных офисных задач можно использовать:

- OpenOffice[22]: крупный офисный пакет, позволяющий обрабатывать текстовые документы, электронные таблицы, презентации, а также создавать растровые и векторные изображения. В достаточной мере совместим с такими форматами M$Office, как `.doc`, `.xls`.
- koffice[23]: офисный пакет, аналогичный по функциональности M$ Office. Также как и OpenOffice, в большой степени совместим по форматам с M$ Office.

Оба этих офисных пакета очень удобны для работы, особенно если создавать в них документы с начала, не таща за собой наследие M$ Office.

12.3. Работа с графикой

- Для рисования растровой графики используется `GIMP`[24]. Это крупный пакет по обработке растровой графики, аналогичный по функциональности `Adobe® Photoshop®`.
- Для векторной графики: oodraw[25], векторный редактор, входящий в состав пакета `OpenOffice.Org`. Чем-то напоминает `Corel® Draw™`
- Сканирование: xsane[26] - мощнейшая утилита для работы со сканером. Имеет множество возможностей и функций. Работает с огромным количеством сканеров. Сканировать изображения можно также из `GIMP`

12.4. Музыка и видео

Пройдемся по утилитам для проигрывания музыки:

- `XMMS`[27]: (X MultiMedia System) программа, аналогичная **WinAMP**. Умеет играть `.wav`, `.mp3`, `.ogg` и множество других форматов. Может проигрывать аудио CD. С помощью xmms можно также просматривать некоторые видео в некоторых форматах. Имеется возможность смены "скинов" и прочие функции, присутствующие в **WinAMP**.
- mpg123[28] простой консольный проигрыватель `mp3`. Удобно использовать в скриптах или при вызове внешней программы. Например, вы можете вызвать `mpg123` при получении нового письма или настроить планировщик задач на выполнение этой программы, проще говоря поставить будильник.
- ogg123[29]: простой консольный проигрыватель Vorbis ogg. Точно такой как mpg123 но только играет ogg вместо mp3.
- grip[30]: программа с графическим интерфейсом для снятия песен с аудио CD. Умеет сразу конвертировать песни в mp3/ogg.

21. http://www.krasu.ru/soft/chuchelo/
22. http://openoffice.org/
23. http://koffice.kde.org/
24. http://www.gimp.org/
25. http://www.openoffice.org/
26. http://www.xsane.org/
27. http://www.xmms.org/
28. http://www.mpg123.de/
29. http://www.vorbis.com/
30. http://www.nostatic.org/grip/

- kmidi[31] Хороший проигрыватель MIDI файлов.

Существует еще множество утилит для проигрывания и редактирования звуковых файлов.

Теперь о просмотре видео:

- mplayer[32]: Очень хороший проигрыватель видео. Знает 44 аудио и 110 видео кодеков. Может просматривать DVD. Может работать как в X, так и в консольном варианте. Может работать даже в текстовом режиме, показывая фильмы с помощью обычных букв. Имеет также свой encoder, позволяющий упаковывать видео в множество форматов, включая DivX и XviD. Этому плееру можно "подложить" декодеры, скомпилированные для M$ Window$ (dll или acx) и он сразу начнет проигрывать формат, декодируемый этим декодером.
- xine[33]: тоже замечательный плеер с красивым интерфейсом. Имеет множество приятных функций. Может проигрывать очень много форматов видео.

31. http://kde.org
32. http://www.mplayerhq.hu/
33. http://xine.sf.net/

Глава 13. Основные ссылки по Mandrake Linux

Ниже приведен список ресурсов, на которые стоит обратить внимание.

- Официальный сайт Mandrake Linux на русском языке: http://mandrakelinux.com/ru/. Это главный источник получения информации по *Mandrake Linux*.
- Официальные списки рассылок Mandrake Linux `expert-ru` и `newbie-ru` : http://mandrakelinux.com/ru/flists.php3 Это официальное сообщество русскоязычных пользователей Mandrake Linux, где можно получить бесплатную поддержку и обсудить интересующие вопросы на тему Mandrake Linux.
- Архив рассылок Mandrake Linux `expert-ru` и `newbie-ru`:
  - http://archives.mandrakelinux.com/newbie-ru
  - http://archives.mandrakelinux.com/expert-ru
- Документация на русском по Linux Mandrake: http://mandrakelinux.com/ru/fdoc.php3.
- Клуб пользователей *Mandrake Linux*: страница Клуба Mandrake на русском http://mandrakelinux.com/ru/club/ и и сайт Клуба (на многих языках) http://www.mandrakeclub.com.
- Рассылка новостей на subscribe.ru, посвященная Linux Mandrake: http://subscribe.ru/catalog/comp.soft.linux.mand

Также приглашаем посетить наш форум поддержки http://Lafox.net/support/, где вы можете оставить свои комментарии и предложения к данному руководству. Спасибо.

Удачи!

Lafox.Net Team